IMPLEMENTATION AND ANALYSIS OF SECURITY SYSTEM IN WIRELESS SENSOR NETWORK BASED ON ZIGBEE STANDARD

[1]JORJIANA AMINATUS SIP, [2]RENDY MUNADI, [3]GUSTOMMY BISONO

[1,2,3]Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Univesitas Telkom
E-mail: [1]jorjiana.asip@gmail.com, [2]rendymunadi@telkomuniversity.ac.id, [3]bisono.telu@gmail.com

Abstract - Wireless Sensor Network (WSN) is a technology that being warmly used both for research and to help human activities. System security is one of the important things that must be considered both in wireless and wire line network. Wireless sensor networks are expanding which are vulnerable and therefore require an effective security mechanism. Wireless sensor networks have several constraints such as limited memory, energy and computational capabilities that create constraints when coupled with security at sensor nodes. To solve the problem, this final project will implement and analyze security system in wireless sensor network refers to ZigBee standard. ZigBee schemes can be synchronized with new protocols targeted at low rates, small power devices, and sensor nodes. ZigBee requires cryptography that is expected to save power, computing power, and storage resources. To that end, the chosen security system is using AES encryption algorithm (Advanced Encryption Standard) which is implemented directly on ZigBee. In this research successfully apply AES128 decryption and encryption algorithm on wireless sensor network. The test used is a passive attack that can only see and capture the package only. In a security performance analysis, the confidentiality parameter is not fulfilled if it does not use security. Integrity parameters are fulfilled using or without security. The largest throughput value is 1122 bytes / s at a distance of 21 meters. And the last delay at a distance of 49.5 meters with a value of 4.1483 s.

Key words - WSN, ZigBee, AES128

I. INTRODUCTION

Wireless Sensor Network (WSN) is a technology used for research as well and to facilitate daily life. WSN is a network infrastructure that can detect, calculate and have communication elements that can transmit data to the administrator to measure, observe, and give orders if there are certain conditions. Wireless sensor is an important aspect of existing network in IoT implementation because the sensors are small portable devices, and can be implemented in many applications [2].

The security system is one of the important things that must be considered both wireless and wired networks. WSN users should believe that the information they receive from the network is reliable, accurate, and not damaged by irresponsible parties. Wireless sensor networks have several constraints such as memory limitations, energy and computational capabilities that create constraints when added to the security of the node sensor. To send information that has been read by the sensor node ZigBee needed to send the information to the user WSN. ZigBee is a standard set in IEEE 802.15.4, consisting of a physical layer (PHY), intermediate access control layer (MAC), network layer (NWK), and application layer [3].

To solve the problem, this research applies and analyzes system security on wireless sensor network refers to ZigBee standard. ZigBee is an emerging standard for low power, low level wireless communications with the goal of both systems being able to work together and can include all devices within the scope of power despite low WSN node sensors [4]. ZigBee requires cryptography which is expected to save power, computing power, and storage resources. The AES encryption algorithm was once performed on IEEE 802.15.4 devices but using TelosB [5]. In the end, the security system is chosen using AES encryption algorithm (Advanced Encryption Standard) which is implemented directly on ZigBee.

II. BASIC THEORY

A. ZigBee

The ZigBee Alliance is supported by members such as Siemens, Philips, Texas Instruments, and Samsung promoting a wireless specification that offers low power communications and short-range medium-to-250kbps data transmission on the 2.4 GHz frequency band. ZigBee is developed by IEEE for low-power remote devices. It also offers a very high security mechanism for protecting the correctness of data through encryption [2]. ZigBee includes common attributes: low performance, short to medium range, low power, and low cost. ZigBee is based on the IEEE 802.15.4-2006 and IEEE 802.15.4-2003 standards, which specify using Direct Sequence Spread Spectrum (DSSS) operations in some unlicensed bands: 868 MHz, 915 MHz, and 2.4 GHz [7].

ZigBee consists of physical layer (PHY), medium access control (MAC) layer, network layer (NWK), and application layer [3]. PHY layer is a function to enable or disable radio transmitter, energy detection (ED), link quality instruction (LQI), idle channel assessment (ICA), channel selection, and data transmission / reception. The MAC layer is responsible to generating network towers,

synchronizing between towers, connecting / disconnecting PANs, providing CSMA-CA access mechanisms, and establishing reliable communications in connecting between MAC peer entities.

ZigBee provides two different security: standard security ie basic security profile, this security is rarely adopted because it can be exposed to attack. And high security, mostly used because it ensures better security during communication. Link keys are one of the security keys adopted by ZigBee [18]:

1) Master Keys are usually hardcoded on device or shared out-of-band. This is necessary in order to retrieve other keys but never directly sent to the network.
2) Network Keys is a key owned by all devices connected to the same network. These keys are generated by the Trust Center and these keys can be sent to the network in plain text or in encrypted form, depending on which security profile is adopted. Network keys are used by all devices to protect all network frames (routing messages, network join requests, etc.) and prevent the incorporation and use of ZigBee networks by unauthorized devices [9].
3) Link Keys are keys generated using the master key and adopted for communication between two different devices and on the same network.

B. AES

AES (Advanced Encryption Standard) is a symmetric chipertext block that can encipher (encipher) and decrypt (decipher) information. Encryption converts data that can no longer be read called ciphertext; otherwise the decryption is to change the ciphertext data into its original form that we know as plaintext. The AES algorithm uses cryptographic keys 128, 192, and 256 bits to encrypt and decrypt data on blocks of 128 bits.

C. Examination Parameters

In this research there are several parameters tested, both on the security side and on the network quality. Below is a general test parameter on the security side. The parameters used in the test on the security performance side of the WSN are [19]:

1) Confidentiality of Information, requires data or information be accessible only to the competent authorities. the nature of wireless communication between sensors and devices eases attacks, moreover there is no strict physical limit of the transmission medium.
2) Integrity of Information, requires that information can only be changed by the authorities. In addition to the confidentiality of information exchanged, its integrity can be threatened by an attacker who adds extra fragments to the packet or manipulates the data.
3) Availability of Information, requires that information should always be available when needed.

While in testing, the quality of the network in addition to testing on the quality of the network research is also testing the signal received each node. Here is the network quality parameters used:

1) Throughput, is the average speed of data received within a certain time interval of observation.

$$Throughput = \frac{frame\ size}{total\ time\ frame\ deltvery} \quad (1)$$

2) Delay, is the length of time it takes the packet when sent by the sender until it is received by the recipient.
3) RSSI (Received Signal Strength Indication), is a parameter that shows the receiving power of all signals in the measured channel frequency band [19]. Usually RSSI is dBm size, which is ten times the power ratio logarithm (P) at the receiving end and the reference power (Pref). The power at the receiving end is inversely proportional to the square of the distance [21].

$$r = 3(RSSI - 91) \quad (2)$$

4) LQI (Link Quality Indication), is a metric introduced in IEEE 802.15.4 that measures errors in incoming packet modulation successfully received. LQI metrics characterize the strength and quality of packets received. These are introduced in the 802.15.4 standard and provided by CC2430. LQI measures each packet successfully received and the resulting integer ranges from 0×00 to 0×ff (0-255), represents the lowest and highest quality signal that can be detected by the receiver (between -100 dBm and 0 dBm) [21]

III. PREVIOUS WORK

The WSN environment may be exposed to Internet-originated attacks such as Denial of Service (DoS), and in this context availability and resilience are important conditions [5]. A secure network uses a trust center, which cares about the key. Secure networks do not use a single-moment lock, but use multiple keys and continuously change keys [10].

Securing a wireless sensor network requires a network that can support all aspects of security: confidentiality, integrity, authenticity, and availability. To choose the most efficient encryption algorithm in all aspects such as speed of operation, storage and power consumption. Symmetric cryptographic keys process faster than cryptography using asymmetric keys. The symmetric key cryptography mechanism uses a shared key between sender and receiver that is used for both encryption and decryption. the symmetric key algorithm can be subdivided the core block ciphers for transformation in plain-text data, and stream ciphers for varying transformation times. Symmetrical cryptographic keys used on wireless sensor networks such as AES, DES, CAST, and RC5 [1].

The ZigBee security mechanism is not a single independent protocol, but a set of security elements on

IEEE 802.15.4. This is for easier realization on weakly computing platforms, therefore AES is selected. Most current ZigBee chips have built-in AES acceleration circuit devices to speed up the process of this mechanism [3]. IEEE 802.15.4 recommends using AES 128-bit encryption scheme [4]. The cryptography in the ZigBee specification is based on the use of 128-bit keys and AES encryption standards. Encryption, integrity, and authentication can be applied to the Application, Network, and MAC layers to secure frames on each layer.

Johnstone et al. [11] has conducted research on the security of WSN using ZigBee CC2400 series chipset device designed by Texas Instrument. And for the attacker using hardware SmartRF04EB Evaluation Board with a CC2430 and CC2430DB.

Olawumi et al. [14] in his description, having performed three series of attacks. The first attack is knowing all ZigBee networks are active within the range and ZigBee device information. The second attack is the attacker tapping network network traffic that is unencrypted or encrypted to obtain and use that information. The third attack is replying the captured data as if the original sender is sending data again.

The parameters used in security performance testing should be two more: Authenticity of Communication Peers and Avaibility of Information, but on J.Market et al. [17] says that attacks with availability and authenticity parameters are still in the topic of future research. So, in this research using two parameters that have been done that is integrity and confidentiality.

RSSI and LQI are one of the test parameters. The values of these two parameters also affect the security of the WSN. The localization system presented in Joana et al. [21] is based on RSSI as an indicator of strength and LQI as an indicator of the quality of packets received and can also be used to estimate the distance from the node to the reference point.

IV. EXAMINATION SCENARIO

There are two testing scenarios of this research that is on the side of network security performance and network quality performance. In this research using passive attacks that only listening and packet capture are transmitted. This research uses three nodes (1 node coordinator, and 2 sensor nodes) as seen in Figure 1.

On the coordinator node side uses Arduino UNO, XBee S2, and LCD to display the results of the sensor nodes. Sensors used are DHT11 sensors and PIR sensors. On the attacker side using hardware Raven USB Stick (RZUSBSTICK) and use AVR Wireless Service software on Windows OS 8.1 and KillerBee firmware on Kali Linux OS. AVR Wireless Service to know the value of RSSI and LQI. While the KillerBee firmware use for packet capture is being transmitted, capture file can be viewed using Wireshark software.

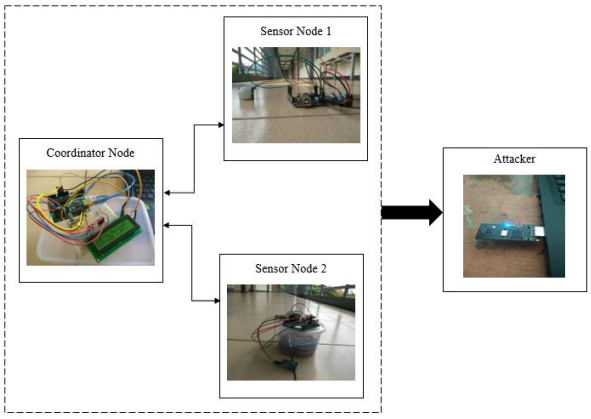


Fig 1. WSN

A. Security System Configuration on XBee S2 Wire Antenna

XBee S2 functions as sender and receiver. In this wireless sensor network, XBee S2 is used as the coordinator and end node to be configured with the help of XCTU software. The third Xbee S2 uses the operating channel from 11-26. On the XBee S2 side itself has three scenarios for security. First without security, both pre-configured link keys, and the third is obataining keys during joining.

Table 1. Coordinator Node

	Non-Security	Pre-configured link keys	Obtaining keys during joining
ID	1235	1235	1235
EE	0	1	1
EO	0	0	1
NK	0	0	0
KY	0	4455	0

Table 2. Sensor Node

	Non-Security	Pre-configured link keys	Obtaining keys during joining
ID	1235	1235	1235
EE	0	1	1
KY	0	4455	0

In the non-security configuration does not activate the security system on the XBee S2 device nor on the Arduino UNO. In this configuration the most important thing is that WSN runs well by giving the same PAN ID on the side of the coordinator as well as on the second side of the sensor nose.

Pre-configured link keys set the same EE, ID, and KY commands on all devices. After successfully joining a

secure network, the network key encrypts all application data transmissions. Since NK is set to 0 in the coordinator, the device selects a random network key. Because KY is configured to non-zero values on all devices, the KY pre-configured key identifier sends an encrypted network key when the device is merged [15].

Whereas, obtaining keys during joining set the same EE, ID, and KY commands on all devices. Since NK is set to 0 in the coordinator, the device selects a random network key. Since KY is set to 0 on all devices, the network key is sent unencrypted when the device is merged. And giving EO the number 1, means making the coordinator as trust center [15].

In the pre-configured system configuration of link keys and obtaining keys during joining on Arduino UNO added coding AES128 encryption algorithm.

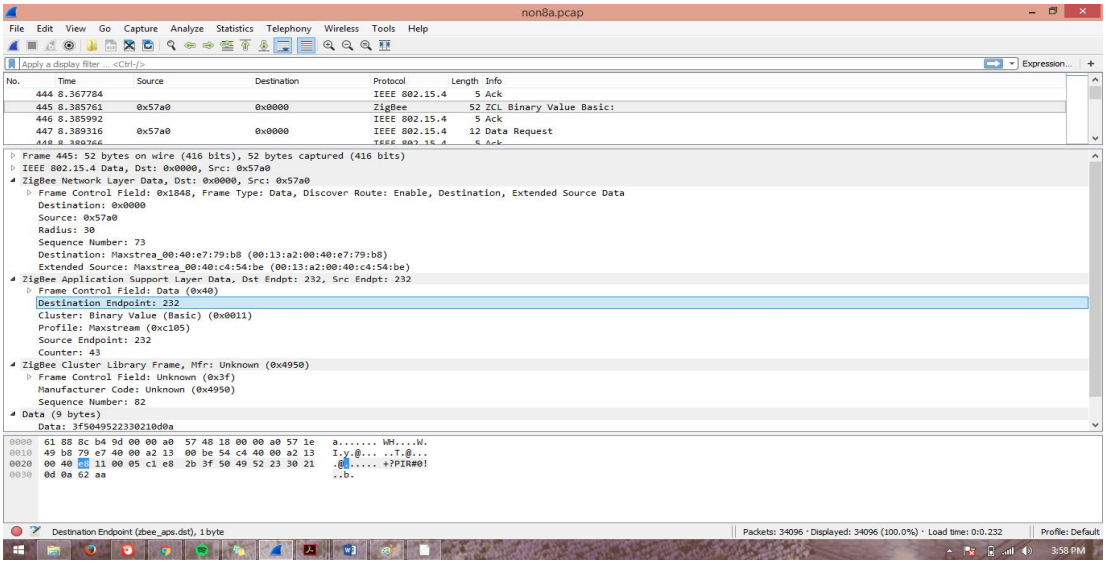
V. RESULT AND ANALYSIS

Testing of this research is on the side of network security performance and network quality performance.

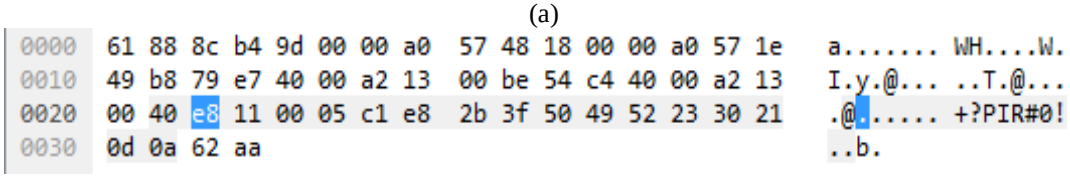
A. Network Security Performance

1) Non-Security

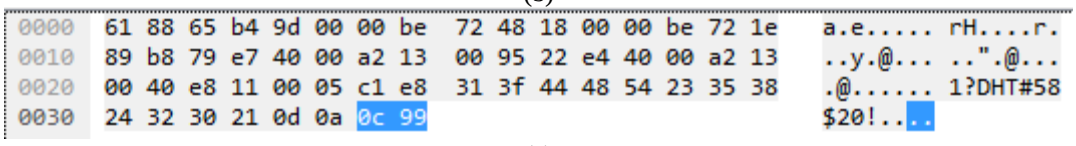
Since most ZigBee networks do not use encryption at all, it makes hackers wanting to eavesdrop on ZigBee network traffic and misusing captured data may contain sensitive information for their own malicious attacks. The different with security or without security is the ZCL (ZigBee Cluster Library) information in Wireshark software (Figure 2a), whereas with no security this information. ZCL serves as a repository for the cluster functionality developed by ZigBee and as a consequence ZCL becomes a working library with regular updates if any new functionalities are added.



(a)



(b)



(c)

Fig 2. (a) ZCL Info on Wireshark (b) PIR's Info (c) DHT's Info

Can be seen in Figure 2a the sender's address is 0x72be and the recipient address is 0x0000. And in FIGS. 2b and 2c explain the existence of data sent from PIR sensor. In ZCL information there is also a manufacturer code which is a code allocated by ZigBee Alliance that connects the manufacturer to the device and for tunneling (factory-specific protocol). And the manufacturer code value in figure 2a is 0x4950. As well as the value of the frame control field ZCL is 0x3f which means that the cluster is reserved (already ordered) [23].

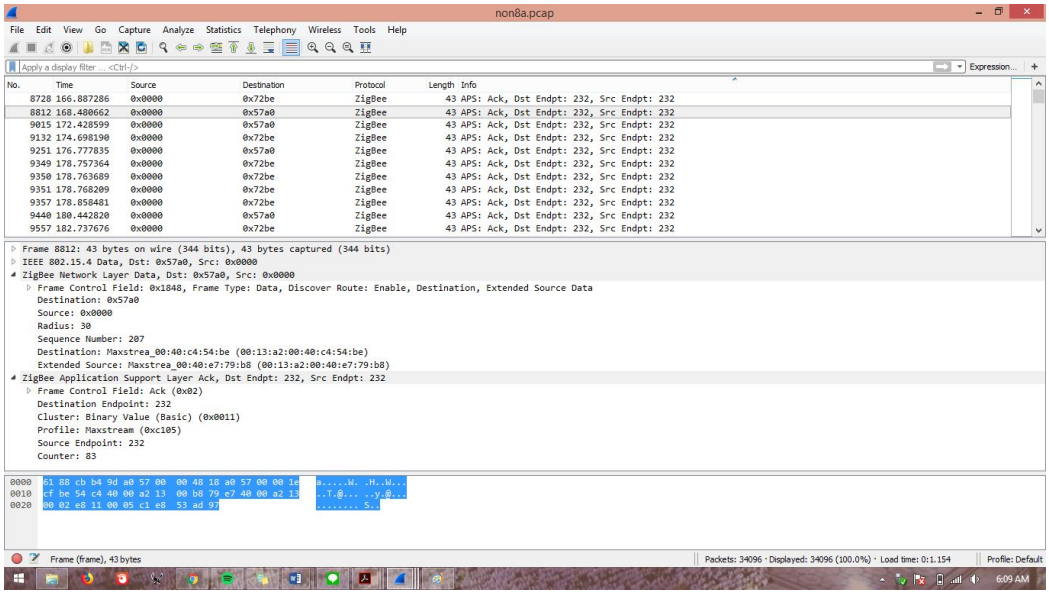


Fig 3. APS's Info

In addition to ZCL information, if doesn't using the security system then, it can be seen information about ZigBee Application Support Data Layer, this is also called APS. APS (Application Support Sublayer) provides the services needed for endpoints and ZDO to interact with the network layer for data and management services. Some services provided by APS for application objects for data transfer are request, confirmation, and response. Furthermore, APS provides communications for applications by defining integrated communications structures (eg, profiles, clusters, or end nodes). In Figure 3 we have a cluster ID value of 0x0011 and APS 0xc105 profile value which means that invalid or out of range parameters have been passed to the primitive of the next higher layer [24].

2) Pre-configured Link Keys

In this condition has been inserted AES128 encryption algorithm on Arduino UNO, so gotten long time process of encryption and decryption. On the DHT11 sensor takes 0.3242s for encryption and 0.481s for decryption. While the PIR sensor takes 0.0393s for encryption and 0.1984s for decryption. After using this security system configuration information in the form of ZCL and APS does not appear, unlike configuration without security.

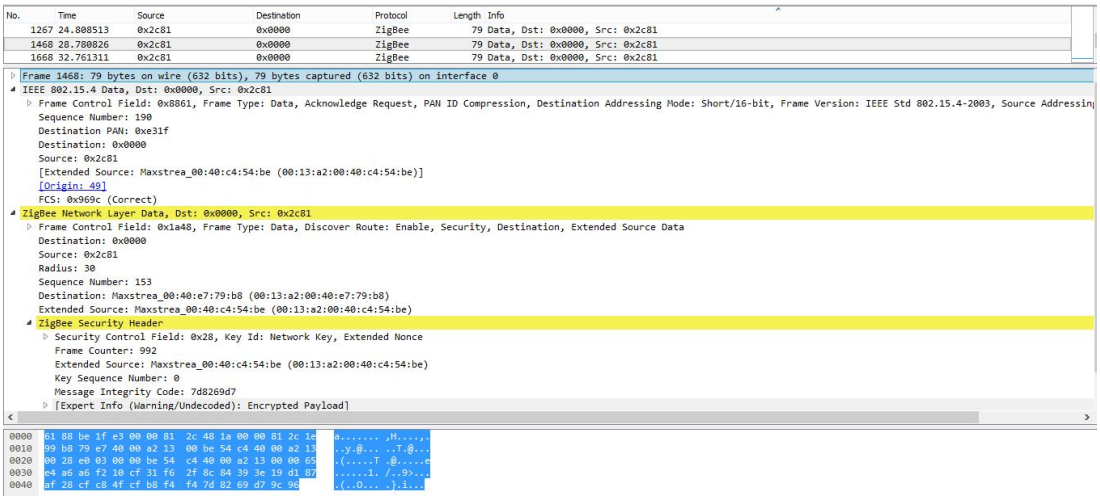


Fig 4. Pre-configured's Data Info

In Figure 4 we can see the zigbee security header which means that in WSN using pre-configured link keys it has activated its security key. On the info it can be seen that we can't see the information sent to the recipient because the data has been encrypted on Arduino Uno module using AES-128. And seen the value of MIC

3) Obtaining keys during joining

In this condition has been inserted AES128 encryption algorithm on Arduino UNO, so gotten long time process of encryption and decryption. On the DHT11 sensor takes 0.322s for encryption and 0.4871s for decryption. While the PIR sensor takes 0.0393s for encryption and 0.1877s for decryption. After using

this security system configuration information in the form of ZCL and APS does not appear, unlike configuration without security.

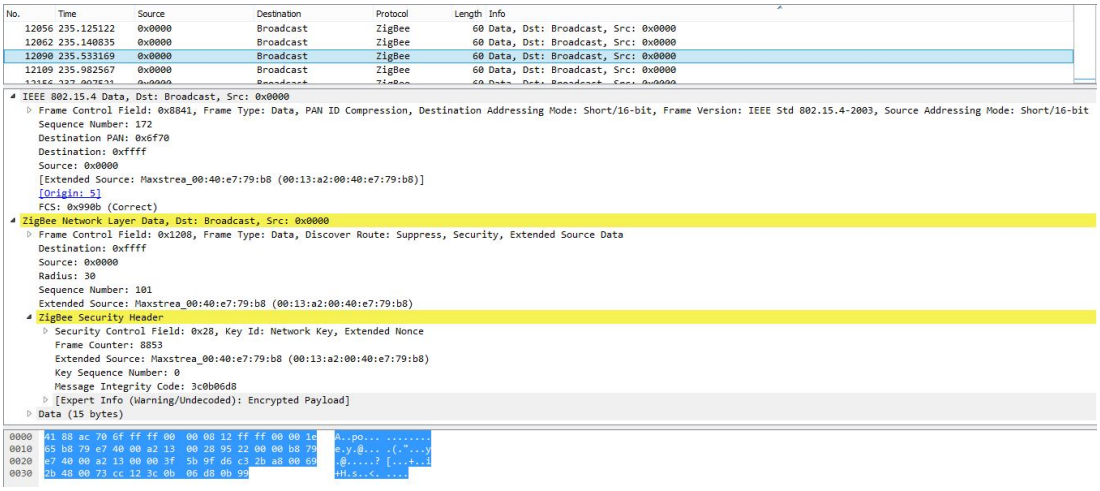


Fig 5. Obtaining's Data Info

In Figure 5 inform the incoming data to the recipient. But we can't see the information sent to the recipient because the data has been encrypted in the Arduino Uno module using AES-128. The AES algorithm is not only used to encrypt information but also to validate the transmitted data.

Network Quality Performance

1) Throughput

This throughput is calculated on the side of the coordinator node connected to the PIR sensor node and DHT11 sensor node. Can be seen from Figure 6 it can be concluded that 25 meters is the optimal distance XBee S2 work. And began to decline at a distance of 30 meters and decreased drastically at a distance of 40 m. As well as the higher throughput, the more power in WSN is used.

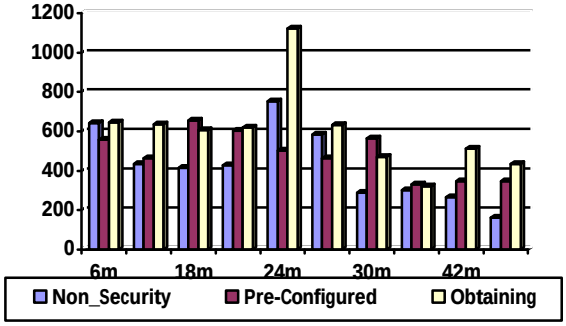


Fig 6. Throughput Graphic

2) Delay

In this delay test is done open room. In figure 7 it can be seen that there is no big difference between the conditions one with other conditions. The further the sensor node the longer the coordinator node receives the data packets from the two sensor nodes. There is no large difference between the conditions with one another, it can be concluded that using or not using AES128 decryption security encryption has no effect in the arrival of information transmitted

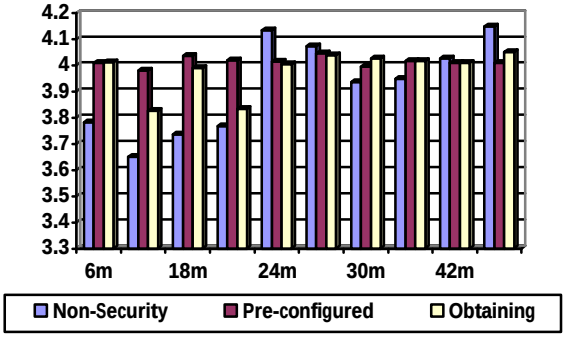


Fig 7. Delay Graphic

3) RSSI

RSSI (Received Signal Strength Indicator) is a parameter that shows the receiving power of all signals in the measured frequency band of the pilot channel. In this test scenario, RSSI gets each node. Figure 8 below shows RSSI on all three nodes. The greatest RSSI lies on the first meter. Node coordinator with RSSI -94,9 dBm, sensor node 1 with RSSI -95,1 dBm, and sensor node 2 with RSSI 92,933 dBm. As well as, in figure 8 showing the RSSI chart, it can be seen the further the sniffer the lower the RSSI.

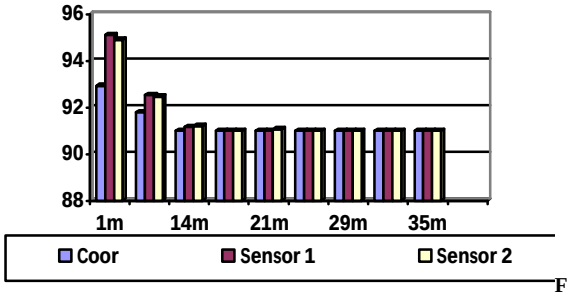


Fig 8. RSSI Graphic

4) LQI

Link Quality Indication (LQI) is a metric used to estimate link quality of RF transmission. As defined in IEEE802.15.4, LQI is calculated by the physical layer and gives signal strength and quality links to the network and above the layer after each frame of data is received. LQI is one of the alternatives used to know the value of RSSI. If the value of RSSI in AVR Wireless Services software has reached the value 0 then we can see the value of LQI, where the value of LQI has a range between 0-255.

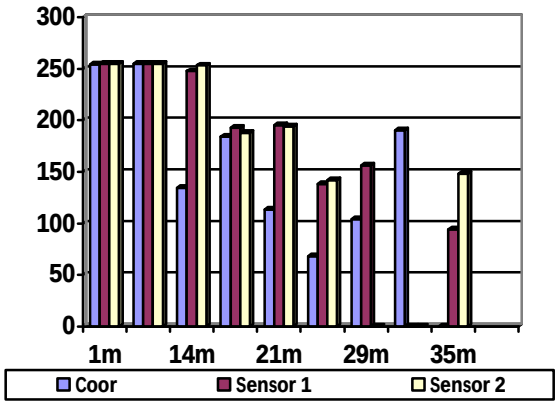


Fig 9. LQI Graphic

In figure 9 can be seen starting at a distance of 29 meters LQI sensor-2 value is not displaying the value, which means there is no communication on the sensor network. And at a distance of 35 meters sensor nodes are still seen the value of RSSI and LQI

CONCLUSIONS

The goal of this research is to successfully implement the security system on wireless sensor network using XBee S2 device. This research successfully implements the security system on WSN using AES128 encryption algorithm. In the security performance analysis it can be concluded that using security is more secure because the sniffer can not see the data sent on the wireless sensor network. Whereas, without security sniffer can see data sent. So it can be concluded that without confidentiality the parameters of confidentiality can not be satisfied and in conditions with security using pre-configured or obtaining parameter confidentiality can be fulfilled. And, the integrity parameters can be met by all the conditions that either use the security or do not use the data security remain intact, it can not be changed because it has implemented the security system configuration and get the MIC (Message Integrity Code).

The value of RSSI and LQI can also affect the security of wireless sensor networks. For example, if the greater the value of RSSI and LQI indicates that there is a ZigBee device nearby. If the sniffer is used for harm to others, then the ZigBee device will be taken and used for malicious purposes.

REFERENCES

[1] Panda, Madhumita. (2015). Data Security in Wireless Sensor Network via AES Algorithm. ISCO. India

[2] Maphats'oe, Ts'itso and Muthoni Masinde. (2016). A security Algorithm for Wireless Sensor Networks in the Internet of Things Paradigm.IST-Africa.South Africa

[3] Yang, Bin. (2009). Study on Security of Wireless Sensor Network Based on ZigBee Standard. International Conference Computational Intelligence and Security. China

[4] Dini, Gianluca and Marco Tiloca. (2010). Considerations on Security in ZigBee Networks.International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing. Italy

[5] Granjal, Jorje., Edmundo Monteiro, and Jorge Sa Silva. (2015). Security for the Internet of Things: A Survey of Existing Protocols and Open Research issues. IEEE Communications Surveys and Tutorials

[6] Candra, Shalahuddin Kartika. "Desain dan Implementasi WSN pada Tempat Sampah dalama Gedung Berbasis Mikrokontroler Menggunakan RF Modul Zigbee dengan Topologi Cluster Tree". Telkom University. Indonesia. 2015

[7] Geier, Jim. "Designing and Deploying 802.11n Wireless Networks". Cisco Press. Indianapolis USA. 2010

[8] Masica, Ken. (2007). Recommended Prectices Guide for Securing ZigBee Wireless Networks in Process Control System Envireonments. DHS US CERT Control Systems Security Program (CSSP). USA

[9] Blonter, Melissa., and Chow Ming. (2015). Smart Home Technology : The ZigBee Protocol. Computer Systems Security. Tufts University. USA

[10] Daemen, Joan., and Vincent Rijmen. "The Design of Rijndael AES – The Advanced Encryption Standard". Springer. Belgium. 2001

[11] Johnstone, Michael N., and Jeremy A. Jarvis. (2011). Penetration of ZigBee-based Wireless Sensor Networks. Australian Information Warfare and Security Conference. Edith Cowan University. Australia

[12] Stelte, Bjorn., and Gabi Dreo Rodosek. (2013). Thwaeting Attacks on ZigBee – Removal of the KillerBee Stinger. IFIP. German

[13] Soleimay, Kiana. (2011). Security in IEEE 802.15.4/zigbee. University of Mazandaran. Iran

[14] Olawumi, Olayemi., Keijo Haataja, Mikko Asikainen, Niko Vidgren, and Pekka Toivanen. (2014). Three Practical Attacks Against ZigBee Security: Attacks Scenario Definitions, Practical Experiments, Countermeasures, and Lesson Learned. IEEE. Finland

[15] Digi International Inc. (2017). "XBee/Xbee-PRO® S2C Zigbee® RF Module". [Online]. Tersedia: https: //www.digi.com/resources/ documentation/DigiDocs/ 90002002/default.htm#Containers accessed on 13th September 2017

[16] Riverloopsec. (2017). "IEEE 802.15.4/ZigBee Security Research Toolkit". [Online]. Tersedia: http://www.riverloopsecurity.com accessed on 20th June 2017

[17] J.Market, M.Massoth, K-P.Fischer-Hellmann, S.M.Furnell, and C.Bolan. (2011). Attack Vectors to Wireless ZigBee Network Communications – Analysis and Countermeasures. Proceedings of SEIN. Germany

[18] Vaccari, Ivan., Enrico Cambiaso, and Maurizio Aiello. (2017). Remotly Exploiting AT Command Attacks on ZigBee Networks. Hindawi. Egypt

[19] Seitz, Andrew., and Benjamin Ramsey. (2016). Z-Ranger : An Improved Tool Set for ZigBee Warwalking. 11th International Conference on Cyber Warfare & Security Boston University. USA

[20] Christin, Delphine., Parag S. Morge, and Matthias Hollick. (2010). Survey on Wireless Sensor Network Technologies for Industrial Automation : The Security and Quality Perspectives. ISSN 1999-5903. German

[21] Joana, Sharly., and Wooju Kim. (2012). A Fusion Approach of RSSI and LQI for Indoor Localization System Using Adaptive Smoothers. Journal of Computer Networks and Communication. South Korea

[22] Wildan Yoga Swara. "Perancangan dan Implementasi Sistem Indoor Localization Berbasis Wireless Sensor Network dengan Perangkat ZigBee". Telkom University. Indonesia. 2016

[23] ZigBee Alliance. "ZigBee Cluster Library Specification Rev.6". (2016)

[24] ZigBee Alliance. "APS ZigBee Specification". (2012)

★★★